

Making Waves Academy

Data Classification Policy and Protection Guidelines

December 10, 2020



Objectives



- Provide an overview of the policy to Board members are aware of its purpose
- Gather input from the Board on any areas requiring adjustment and to identify any gaps in the policy
- Provide clarity and information for the Board on any questions they have
- Obtain Board approval for the policy

Purpose



- The purpose of the Data Classification Policy and Protection Guidelines is to establish a framework for generally classifying organizational and educational data based on its level of sensitivity, value, and criticality to MWA. It also sets out how to handle and protect data based on how it is classified.

Overview



- **Compliance:**
 - The policy is aligned with state and federal laws
 - The policy is aligned with other MWA policies
 - The policy was developed and vetted by our attorney
- **Policy Data Classifications:**
 - ***Protected Data*** - Information that is protected by statutes, regulations, MWA policies and procedures or other contractual language, i.e. student records. This data shall not be disclosed to unauthorized individuals, agencies or external sources except as specifically authorized by law.
 - ***Sensitive Data*** - Highly confidential or personal information which, if breached or disclosed to unauthorized persons, could result in legal liability, fines, penalties, theft and/or fraud.
 - ***Public Data*** - Information that may be disclosed to any person regardless of their affiliation with MWA i.e. press releases on our website.

Overview (continued)



- **Requirements for Protection:**

- ***Public Data*** – Can be shared broadly both internally and externally. This data requires little protective measures, except to ensure that it cannot be modified by unauthorized personnel.
- ***Protected Data and Sensitive Data*** – Specific guidelines, outlined in the policy, must be followed and include but are not limited to collecting, accessing, sharing, handling and storing data.

Advantages of Establishing the Policy



- Ensures Faculty and Staff have a clear set of guidelines to reference on how to store and handle data.
- Ensures IT Staff have a clear set of guidelines on how to setup and maintain access to data.
- Ensures Leadership, Managers and Supervisors have a clear sense of how to hold those they lead accountable for managing and handing data specific to their area.

Goals and Next Steps



- **Goals:**

- In January, utilize this policy to inform a project plan to begin utilizing cloud data storage (like Google drive) securely and responsibly.
- Roll out the policy to staff and faculty this Spring, along with communicating a plan around use of Google drive or, other Cloud based data storage solutions.

- **Next Steps:**

- Work with stakeholders to identify data owners to begin classifying data and identify storage and sharing requirements.
- Work with the IT Team to develop systems, processes and technology or services that may be utilized for data storage and sharing.

Key Questions



- Were there any parts of the policy that require further clarification?
- Was anything missing from or, are there any adjustments needed?
- Can the policy be approved as is, or should I present another draft that includes input gathered today?